

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade



U.S. Customs and Border Protection

Statement of Work (SOW)

For

**Splunk Enterprise Logging Maintenance Renewal & Upgrade
PR# 20085933**

March 4, 2016

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

Table of Contents

1	BACKGROUND	1
2	SCOPE/Description of requirements	1
3	APPLICABLE DOCUMENTS.....	3
4	SPECIFIC TASKS.....	3
5	DELIVERABLES AND DELIVERY SCHEDULE	5
6	GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION	6
7	PERIOD OF PERFORMANCE.....	6
8	SECURITY	6
9	SPECIAL CONSIDERATIONS.....	6
10.	Communication Instructions between Contractor and Government	8
	Addendum A.....	10
	Addendum B.....	12

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

1 BACKGROUND

The Customs and Border Protection (CBP), Office of Information and Technology (OIT) is responsible for providing an organization-wide program to ingest, correlate, analyze and report security event data in real time for internal and external threat management. Security Information and Event Management (SIEM) technology provides these capabilities through the collection and recording of event data produced by security sensors.

OIT, Enterprise Network Service Branch (ENSB) seeks this procurement to renew the current maintenance of the OIT Enterprise Logging Solution supporting the operations of all CBP OIT Program Offices. This OIT-funded project provides the necessary capabilities to comply with the Department of Homeland Security (DHS), Office of Management and Budget (OMB), and Congress for the Federal Information Security Management Act (FISMA) reporting and security auditing regulations.

The initial plan presented and approved in Q2/3 FY14 was to implement a SIEM replacement first and ingest only Security relevant data. The approved five year plan would be enacted for implementing an enterprise logging solution and ingesting additional types of data at a later date. Based on this initial approach, it was determined a 1.2TB license would be sufficient to accommodate the expected daily ingestion rate for Security relevant data.

The FY15 Cyber Hygiene efforts directly impacted the scope of the OIT Enterprise Logging Solution which was expanded over multiple occasions to incorporate additional data from any and all available data sources/types. As the result, an upgrade to an unlimited Splunk license is required.

2 SCOPE/DESCRIPTION OF REQUIREMENTS

The purpose of this delivery order is for the contractor to provide the following renewal and upgrade for licenses and support:

MFG P/N	Manufacturer	Description	QTY
		ENTSD/ENSB	
SE-PESUP- R	SPLUNK	Splunk Enterprise - Enterprise Support Renewal- (Existing License Size = 1200 GB/day ; Entitlement = SPL-14146819) Splunk, Inc Start Date: 06/09/2016 End Date: 06/08/2017	1

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

ES-PESUP- R	SPLUNK	Splunk Enterprise Security - Enterprise Support Renewal (Existing License Size = 1200 GB/day ; Entitlement = ESS- 14141704) Splunk, Inc Start Date: 06/09/2016 End Date: 06/08/2017	1
VM-PESUP- R	SPLUNK	Splunk App for VMware - Enterprise Support Renewal (Existing License Size = 100 GB/day ; Entitlement = VMW- 14144281 Splunk, Inc Start Date: 06/09/2016 End Date: 06/08/2017	1
		TASPO	
SE-PESUP- R	SPLUNK	Splunk Enterprise - Enterprise Support Renewal- 100GB Splunk, Inc Start Date: 06/09/2016 End Date: 06/08/2017	1
		WSPD	
SE-PESUP- R	SPLUNK	Splunk Enterprise - Enterprise Support Renewal (Existing License Size = 5 GB/day ; Entitlement = SPL-14136966) Splunk, Inc Start Date: 09/20/2016 End Date: 06/08/2017	1
		Enterprise Unlimited	
YEAR 1			
SE-P-LIC	SPLUNK	Splunk Enterprise - Perpetual License - 10,000GB/day Splunk, Inc	1
SE-P-ESUP	SPLUNK	Splunk Enterprise - Enterprise Support Splunk, Inc	1
SE-T-LIC-ESUP	SPLUNK	Splunk Enterprise - Term License with Enterprise Support - Unlimited- 365 Days Splunk, Inc	1
ES-P-LIC	SPLUNK	Splunk Enterprise Security - Perpetual License- 10,000GB/day Splunk, Inc	1
ES-P-ESUP	SPLUNK	Splunk Enterprise Security - Enterprise Support Splunk, Inc	1
ES-T-LIC-ESUP	SPLUNK	Splunk Enterprise Security - Term License with Enterprise Support - Unlimited- 365 days Splunk, Inc	1
AS-NAM-SAE	SPLUNK	Splunk Advisory Services - Named Advisory Engineer Splunk, Inc	1
EDU-UNIT-1	SPLUNK	Education service UnitSplunk, Inc	100
PS-DEP-US-5	SPLUNK	Splunk Professional Services Deployment, 5 Days Splunk, Inc	20

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

YEAR 2			
SE-P-ESUP	SPLUNK	Splunk Enterprise - Enterprise Support Splunk, Inc	1
ES-P-ESUP	SPLUNK	Splunk Enterprise Security - Enterprise Support Splunk, Inc	1
SE-T-LIC-ESUP	SPLUNK	Splunk Enterprise - Term License with Enterprise Support - Unlimited- 365 Days Splunk, Inc	1
ES-T-LIC-ESUP	SPLUNK	Splunk Enterprise Security - Term License with Enterprise Support - Unlimited- 365 days Splunk, Inc	1
AS-NAM-SAE	SPLUNK	Splunk Advisory Services - Named Advisory Engineer Splunk, Inc	1

3 APPLICABLE DOCUMENTS

The Federal Acquisition Regulation: <http://www.acquisition.gov/FAR/>

Section 508 of the Rehabilitation Act: <http://www.section508.gov/>

Homeland Security Acquisition Regulation (HSAR)
<http://www.dhs.gov/xlibrary/assets/opnbiz/cpo-acquisition-regulation-0606.pdf>

Code of Federal Regulations (CFR): <http://www.gpoaccess.gov/cfr/index.html>

Federal Information Security Management Act of 2014 (FISMA)

NIST SP 800-53, Recommended Security Controls for Federal Information Systems

CBP Information Systems Security Policies (CBP 1400-05x) and Procedures Handbook.

DHS Sensitive System Policy Directive 4300A

DHS Sensitive System Handbook

4 SPECIFIC TASKS

The Contractor shall complete the following tasks as required to comply with this SOW.

4.1 Management

The Contractor shall:

- Provide a single Point of Contact for management of this order

U.S. Customs and Border Protection

Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

- Provide all media commodities as listed on the purchase / delivery order
- Coordinate with the CBP appointed OIT Local Property Officer (LPO) (listed in Shipping Address below) regarding the delivery schedule throughout the duration of the contract effort
- Provide in each physical shipment a report of all product included in the shipment, to include for each device:
 - Contract Line Item Number (CLIN)
 - Description
 - Serial / License number

4.2 Advisory Engineer Professional Services and Education Services

Splunk Advisory Engineer (NAE)

- An NAE is an extension of Splunk technical support and maintenance, commonly known as a technical account manager.
- One NAE will be available to CBP 2 days each week.
- The NAE is part of the technical support services included with this BOM.
- NAE will focus his/her time on assessments of infrastructure and configurations, deployment optimization, on boarding of users, data, reports and use cases, escalation management of support issues, streamlining the coordination of Splunk resources, product deep dives, roadmap discussion, implementation of best practices for the products and use cases, and technical health checks and reporting.

Education Services

- Splunk training for users in the form of virtual or classroom setting.
- Delivery form factor for these are either instructor-led or individual eLearning.
- 100 Training Credits are included in the BOM.
- Training credits can be used at any time and be used by any individuals supporting Splunk at CBP.
- Training material ranges from Splunk for Beginners to Splunk for Advanced Experts.
- Credits can be used towards Splunk Certifications in Splunk product categories.
- Courses range from 1-5 credits per individual.

4.3 Splunk Enterprise Support

The Contractor shall:

- Provide 24x7 technical support and maintenance for the software to include software updates and upgrades.
- Support will be remotely delivered via telephone support, online documentation, and web forums using email and a web-based portal for submitting and tracking

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade
cases.

- This support does not include FTEs, nor is it on-site.

4.4 Splunk Professional Services

- One FTE onsite who will assist with configuring and deploying Splunk solutions.
- Breakdown of units: 5 days = 1 Unit – 20 Units quoted for a total of 100 days included with the BOM. This is 1 dedicated FTE for CBP from Splunk that is onsite and will assist with configuring and deploying Splunk solutions contained in the BOM.
- Virtual deployments can be accepted as well. The FTE will work with each individual CBP program to clearly identify the goals to achieve in deploying Splunk and will assist in the actual deployment and post-deployment to ensure 100% satisfaction and success.

4.5 Monthly Status Reports

The Contractor shall:

Provide a monthly status reports that includes but is not limited to:

- Dates and hours of training/education performed
- Remaining training/education vouchers/hours to be used
- Names of attendees
- Professional services will provide government personnel with product oversight and guidance.

Reports must be submitted to the Contracting Officer's Representative (COR) by Close of Business (COB) the first Monday of every month.

5 DELIVERABLES AND DELIVERY SCHEDULE

5.1 Roles and Responsibilities Matrix

The Contractor shall deliver a completed RRM, as presented in the chart below, to the COR no later than 10 days after date of award. The RRM should include prime and sub-contractor, if applicable, points of contact to ensure communications are routed correctly.

Name	Organization	Role	Responsibility	Phone	Email

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

5.2 Data

The Contractor shall provide copies of any and all documents related to the product(s) and /or support. One copy of the data will be delivered in paper form and another electronically, using Microsoft Word or Adobe Acrobat. The documents are deliverables under the contract and shall be delivered to the COR no later than thirty days after contract award.

6 GOVERNMENT-FURNISHED EQUIPMENT AND INFORMATION

Government furnished equipment is not anticipated under this award. The Contractor will be required to sign a Non-Disclosure Agreement (NDA) for any Government Furnished Information.

7 PERIOD OF PERFORMANCE

The order shall consist of a base period of 12 months, 06/16/2016-06/15/2017 and an optional period of 12 months, 06/16/2017-06/15/2018.

8 SECURITY

There are no specific security classification level requirements associated with this procurement action. Information is deemed unclassified.

9 SPECIAL CONSIDERATIONS

9.1 Delivery Inspection and Acceptance

The Government reserves the right to reject any deliverable based on defects with respect to timeliness and completeness of delivery. In the event of a rejection of any deliverable, the Contracting Officer (CO) will notify the Contractor in writing within five (5) business days of the receipt of the deliverable of any deficiencies to be corrected. The Contractor shall have five (5) business days after notification to correct the deficiencies.

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

9.2 Task Order Administration

COR:

(b) (6)

Name	Title	Office	Telephone	E-Mail Address	Role
(b) (6)	Technical POC	OIT/ENTSD/ENSB	(b) (6)		Reviewer
	Technical POC	OIT/ENTSD/ENSB			Reviewer
	Technical POC	OIT/ENTSD/ENSB			Reviewer

9.3 Terms and Conditions Reference

See Addendum B

9.4 Invoicing

The Contractor shall submit invoices for product shipped and for the maintenance costs. Invoices shall be electronically transmitted to the COR as listed in section 9.2, to ENSBBudgetAndAcquisitions@cbp.dhs.gov and to the National Finance Center (NFC) and CBPinvoices@dhs.gov.

- Order number
- Description of services provided for a specified time period.
- Unit price and total amount of each item.
- Discount terms
- Company name, telephone number, taxpayer's identification number, and complete mailing address to which payment will be mailed.

Only the CO has the authority to represent the Government in cases where the task order requires a change in the terms and conditions, delivery schedule, scope of work and/or price of the products and/or services under this task order.

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

10. COMMUNICATION INSTRUCTIONS BETWEEN CONTRACTOR AND GOVERNMENT

The Contractor listed in the RRM and Government personnel will follow the instructions below for communications:

1. Any communications written or verbal involving modifications to the existing contract must include the Contracting Officer (CO), Contractor Project Manager (PM) and the Contracting Officer's Representative (COR). Reference section 10.1.2.
2. Any written communications must include the Contractor PM and the COR but do not need to be directed to them (i.e. CCing them on emails). These written communications can be directed toward the technical and support specialists listed in the RRM as needed.
3. Phone calls can be made directly between Customs and Border Protection (CBP) and the Contractor PM as needed to exchange information, ask questions, and further discussions as they apply to the roles laid out in the RRM.
4. All support should be directed to the technical and support specialist while CCing the Contractor PM in RRM and COR.
5. All questions should be directed towards the corresponding specialists at identified in the RRM.
6. If unsure of whom to contact regarding a specific issue please reach out to the Contractor PM or the COR for further instructions.

Any communication between Contractor and Government shall not constitute a change of scope for this order. Only the CO can modify this contract.

The COR's primary duty is to monitor the Contractor's performance to ensure that all of the technical requirements under the contract are met by the delivery date or within the period of performance, and at the price of within the estimated cost stipulated in the contract. These include but are not limited to:

- Perform surveillance of the performance under the contract and conduct inspections necessary to ensure performance and compliance with the terms and conditions of the agreement.
- Resolve day-to-day matters within the scope of your authority.
- Assist the contractor in interpreting the terms and conditions or performance requirements, provided that any interpretation or clarification is within the limitations prescribed within this delegation.
- Immediately bring to the contractor's attention, any potentially hazardous working conditions. The contractor is always required to comply with Federal Occupational Safety and Health Administration (OSHA) guidelines, applicable labor and environmental laws, as well as any state or local requirements for workplace safety, whether in a Federal facility or other location. In addition, ensure that the contractor adheres to any specific safety clauses and/or the safety plan in the Contract/Order/Agreement.

U.S. Customs and Border Protection

Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

- Immediately alert the CO to any possible contractor deficiencies or questionable practices so that corrections can be made before the problems become significant.
- Advise the CO of the following situations:
 - Possible changes in contractor management and/or key personnel;
 - Potential labor disputes or workforce problems;
 - Disagreements with the contractor regarding the Statement of Work or Statement of Objectives or Performance Work Statement (SOW or SOO or PWS) requirements or other potential disputes with the contractor about technical or other business matters;
 - Lack of performance that may jeopardize the cost or required schedule of the business agreement.
- Review Contractor requests for travel, overtime, Government assets, or subcontracting in a timely manner and forward to the CO for approval.
- Review and analyze the contractor's deliverables, service, and management reports.
- Provide feedback on contractor performance in CPARS.

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

ADDENDUM A

Acronyms Table

AAA	Authentication, Authorization and Accounting
API	Application Programming Interface
ATS	Address Translation Services
BIOS	Basic Input/Output System
BOM	Bill of Materials
CBP	Customs and Border Protection
CD-ROM	Compact Disk – Read Only Memory
CFR	Code of Federal Regulations
CLI	Command Line Interface
CO	Contracting Officer
COB	Close of Business
COR	Contracting Officer’s Representative
DCBX	Data Center Bridging Capability Exchange
DDR	Double Data Rate
DIACAP	Department of Defense Information Assurance C&A Process
DMA	Direct Memory Access
DOA	Date of Award
DVD	Digital Versatile Disc
ENSB	Enterprise Network Service Branch
ENTS	Enterprise Networks and Technology Support
FAR	Federal Acquisition Regulation
FC	Fibre Channel
FCOE	Fibre Channel over Ethernet
FCP	Fibre Channel Protocol
FISMA	Federal Information Security Management Act
FLOGI	Fabric Login
GB	Gigabyte
Gbps	Gigabits Per Second
GUI	Graphical User Interface
HBA	Host Bus Adapter
vHBA	Virtual Host Bus Adapter
HDD	Hard Disk Drive
HSAR	Homeland Security Acquisition Regulation
IO	Input/Output
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

IT	Information Technology
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPO	Local Property Officer
LUN	Logical Unit Number
MAC	Media Access Control
MTU	Maximum Transmission Unit
NDC	National Data Center
NFC	National Finance Center
NIC	Network Interface Card
NLECC	National Law Enforcement Communications Center
NUMA	Non-uniform Memory Access
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
OS	Operating System
PCIe	Peripheral Component Interconnect Express
PLOGI	Port Login
PXE	Preboot eXecution Environment
QoS	Quality of Service
RAID	Redundant Array of Independent Disks
RADIUS	Remote Authentication Dial-In Service
RAS	Reliability, Availability, and Serviceability
SAN	Storage Area Network
iSCSI	Internet Small Computer System Interface
SCSI	Small Computer System Interface
SIEM	Security Information and Event Management
SOW	Statement of Work
TACACS+	Terminal Access Controller Access-Control System Plus
USB	Universal Serial Bus
UUID	Universally Unique IDentifier
VLAN	Virtual Local Area Network
vNIC	Virtual Network Interface Card
WMI	Windows Management Instrumentation
WWN	World Wide Name
WWNN	World Wide Node Name
WWPN	World Wide Port Name
XML	eXtensible Markup Language

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade
ADDENDUM B

Terms and Conditions Reference

CBP Enterprise Architecture Compliance

The Offeror shall ensure that the design conforms to the Department of Homeland Security (DHS) and Customs and Border Protection (CBP) Enterprise Architecture (EA), the DHS and CBP Technical Reference Models (TRM), and all DHS and CBP policies and guidelines (such as the CBP Information Technology Enterprise Principles and the [DHS Service Oriented Architecture - Technical Framework](#)), as promulgated by the DHS and CBP Chief Information Officers (CIO), Chief Technology Officers (CTO) and Chief Architects (CA).

The Offeror shall conform to the Federal Enterprise Architecture (FEA) model and the DHS and CBP versions of the FEA model, as described in their respective EAs. All models will be submitted using Business Process Modeling Notation (BPMN 1.1 or BPMN 2.0 when available) and the CBP Architectural Modeling Standards. Universal Modeling Language (UML2) may be used for infrastructure only. Data semantics shall be in conformance with the National Information Exchange Model (NIEM). Development solutions will also ensure compliance with the current version of the DHS and CBP target architectures.

Where possible, the Offeror shall use DHS/CBP approved products, standards, services, and profiles, as reflected by the hardware, software, application, and infrastructure components of the DHS/CBP TRM/standards profile. If new hardware, software, or infrastructure components are required to develop, test, or implement the program, these products will be coordinated through the DHS and CBP formal Technology Insertion (TI) process (to include a trade study with no less than four alternatives, one of which reflecting the status quo and another reflecting multi-agency collaboration). The DHS/CBP TRM/standards profile will be updated as TIs are resolved.

All developed solutions shall be compliant with the Homeland Security (HLS) EA.

All IT hardware and software shall be compliant with the HLS EA.

Compliance with the HLS EA shall be derived from and aligned through the CBP EA.

Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval, and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

Development of data assets, information exchanges, and data standards will comply with the DHS Data Management Policy MD 103-01. All data-related artifacts will be developed and validated according to DHS Data Management Architectural Guidelines.

Applicability of Internet Protocol version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS EA (per OMB Memorandum M-05-22, August 2, 2005), regardless of whether the

U.S. Customs and Border Protection

Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

acquisition is for modification, upgrade, or replacement. All EA related component acquisitions shall be IPv6 compliant, as defined in the USGv6 Profile (NIST Special Publication 500-267) and the corresponding declarations of conformance, defined in the USGv6 Test Program.

When a contractor, on the behalf of CBP, handles Sensitive PII data, stores and transmits, the contractor will Accredited (ATO) this information system to the (HHM) FIPS level

DHS Enterprise Architecture Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures. Specifically, the contractor shall comply with the following HLS EA requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware and software shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
- Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
- Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
- Applicability of Internet Protocol Version 6 (IPv6) to DHS-related components (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

OAST (Office on Accessible Systems and Technology) Compliance

DHS Accessibility Requirements Tool (DART)

1 Accessibility Requirements (Section 508)

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology (EIT), they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

All EIT deliverables within this work statement shall comply with the applicable technical and functional performance criteria of Section 508 unless exempt. Specifically, the following

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade
applicable EIT accessibility standards have been identified:

Section 508 Applicable EIT Accessibility Standards

36 CFR 1194.21 Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web based applications as described within 36 CFR 1194.22.

36 CFR 1194.22 Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous Javascript and XML (AJAX) then 1194.21 Software standards also apply to fulfill functional performance criteria.

36 CFR 1194.24 Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available.

36 CFR 1194.31 Functional Performance Criteria, applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.

36 CFR 1194.41 Information Documentation and Support applies to all documents, reports, as well as help and support services. To ensure that documents and reports fulfill the required 1194.31 Functional Performance Criteria, they shall comply with the technical standard associated with Web-based Intranet and Internet Information and Applications at a minimum. In addition, any help or support provided in this work statement that offer telephone support, such as, but not limited to, a help desk shall have the ability to transmit and receive messages using TTY.

Section 508 Applicable Exceptions

Exceptions for this work statement have been determined by DHS and only the exceptions described herein may be applied. Any request for additional exceptions shall be sent to the COTR and determination will be made in accordance with DHS MD 4010.2. DHS has identified the following exceptions that may apply: 36 CFR 1194.3(b) Incidental to Contract, all EIT that is exclusively owned and used by the contractor to fulfill this work statement does not require compliance with Section 508. This exception does not apply to any EIT deliverable, service or item that will be used by any Federal employee(s) or member(s) of the public. This exception only applies to those contractors assigned to fulfill the obligations of this work statement and for the purposes of this requirement, are not considered members of the public.

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

Section 508 Compliance Requirements

36 CFR 1194.2(b) (COTS/GOTS products), When procuring a product, each agency shall procure products which comply with the provisions in this part when such products are available in the commercial marketplace or when such products are developed in response to a Government solicitation. Agencies cannot claim a product as a whole is not commercially available because no product in the marketplace meets all the standards. If products are commercially available that meets some but not all of the standards, the agency must procure the product that best meets the standards. When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, and from that list of products or services, an analysis that the selected product met more of the accessibility requirements than the non-selected products as required by FAR 39.2. Any selection of a product or service that meets less accessibility standards due to a significant difficulty or expense shall only be permitted under an undue burden claim and requires authorization from the DHS Office of Accessible Systems and Technology (OAST) in accordance with DHS MD 4010.2.

All tasks for testing of functional and/or technical requirements must include specific testing for Section 508 compliance, and must use DHS Office of Accessible Systems and Technology approved testing methods and tools. For information about approved testing methods and tools send an email to accessibility@dhs.gov.

ISO Terms and Conditions for Sensitive but Unclassified Requests

DHS Security Policy Requirement

All hardware, software, and services provided under this task order must be compliant with DHS 4300A DHS Sensitive System Policy and the DHS 4300A Sensitive Systems Handbook.

Encryption Compliance Requirement

1. FIPS 197 (Advanced Encryption Standard (AES)) 256 algorithm and cryptographic modules that have been validated under FIPS 140-2.
2. National Security Agency (NSA) Type 2 or Type 1 encryption.
3. Public Key Infrastructure (PKI) (see paragraph 5.5.2.1 of the Department of Homeland Security (DHS) IT Security Program Handbook (DHS Management Directive (MD) 4300A) for Sensitive Systems).

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade
Security Review Requirement

Security Review

The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS, including the organization of the DHS Office of the Chief Information Officer, the Office of the Inspector General, authorized Contracting Officer's Technical Representative (COR), and other government oversight organizations, access to the Contractor's facilities, installations, operations, documentation, databases and personnel used in the performance of this contract. The Contractor will contact the DHS Chief Information Security Officer to coordinate and participate in the review and inspection activity of government oversight organizations external to the DHS. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability and confidentiality of DHS data or the function of computer systems operated on behalf of DHS, and to preserve evidence of computer crime.

Interconnection Security Agreement (ISA)

Interconnection Security Agreement Requirements

Interconnections between DHS and non-DHS IT systems shall be established only through controlled interfaces and via approved service providers. Connections with other Federal agencies shall be documented based on interagency agreements; memoranda of understanding, service level agreements or interconnect service agreements.

Required Protections for DHS Systems Hosted in Non-DHS Data Centers

Security Authorization

A Security Authorization of any infrastructure directly in support of the DHS information system shall be performed as a general support system (GSS) prior to DHS occupancy to characterize the network, identify threats, identify vulnerabilities, analyze existing and planned security controls, determine likelihood of threat, analyze impact, determine risk, recommend controls, perform remediation on identified deficiencies, and document the results. The Security Authorization shall be performed in accordance with the DHS Security Policy and the controls provided by the hosting provider shall be equal to or stronger than the FIPS 199 security categorization of the DHS information system.

At the beginning of the contract, and annually thereafter, the contractor shall provide the results of an independent assessment and verification of security controls. The independent assessment and verification shall apply the same standards that DHS applies in the Security Authorization Process of its information systems. Any deficiencies noted during this assessment shall be provided to the COR for entry into the DHS' Plan of Action and Milestone (POA&M) Management Process. The contractor shall use the DHS' POA&M process to document planned remedial actions to address any deficiencies in information security policies, procedures, and practices, and the completion of those

U.S. Customs and Border Protection
Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

activities. Security deficiencies shall be corrected within the timeframes dictated by the DHS POA&M Management Process. Contractor procedures shall be subject to periodic, unannounced assessments by DHS officials. The physical aspects associated with contractor activities shall also be subject to such assessments.

On a periodic basis, the DHS and its Components, including the DHS Office of Inspector General, may choose to evaluate any or all of the security controls implemented by the contractor under these requirements. Evaluation could include, but it not limited to vulnerability scanning. The DHS and its Components reserve the right to conduct audits at their discretion. With ten working days' notice, at the request of the Government, the contractor shall fully cooperate and facilitate in a Government-sponsored security control assessment at each location wherein DHS information is processed or stored, or information systems are developed, operated, maintained, or used on behalf of DHS, including those initiated by the Office of the Inspector General. The government may conduct a security control assessment on shorter notice (to include unannounced assessments) determined by DHS in the event of a security incident.

Enterprise Security Architecture

The contractor shall utilize and adhere to the DHS Enterprise Security Architecture in accordance with applicable laws and DHS policies to the satisfaction of the DHS COR. Areas of consideration could include:

1. Use of multi-tier design (separating web, application and data base) with policy enforcement between tiers
2. Compliance to DHS Identity Credential Access Management (ICAM)
3. Security reporting to DHS central control points (i.e. the DHS Security Operations Center (SOC) and integration into DHS Security Incident Response
4. Integration into DHS Change Management (for example, the Infrastructure Change Control Board (ICCB) process)
5. Performance of activities per continuous monitoring requirements

Continuous Monitoring

The contractor shall participate in DHS' Continuous Monitoring Strategy and methods or shall provide a Continuous Monitoring capability that the DHS determines acceptable. The DHS Chief Information Security Officer (CISO) issues annual updates to its Continuous Monitoring requirements via the Annual Information Security Performance Plan. At a minimum, the contractor shall implement the following processes:

1. Asset Management
2. Vulnerability Management
3. Configuration Management
4. Malware Management

U.S. Customs and Border Protection

Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

5. Log Integration
6. Security Information Event Management (SIEM) Integration
7. Patch Management
8. Providing near-real-time security status information to the DHS SOC

Specific Protections

Specific protections that shall be provided by the contractor include, but are not limited to the following:

Security Operations

The Contractor shall operate a SOC to provide the security services described below. The Contractor shall support regular reviews with the DHS Information Security Office to coordinate and synchronize the security posture of the contractor hosting facility with that of the DHS Data Centers. The SOC personnel shall provide 24x7x365 staff to monitor the network and all of its devices. The contractor staff shall also analyze the information generated by the devices for security events, respond to real-time events, correlate security device events, and perform continuous monitoring. It is recommended that the contractor staff shall also maintain a trouble ticket system in which incidents and outages are recorded. In the event of an incident, the contractor facility SOC shall adhere to the incident response plan.

Computer Incident Response Services

The Contractor shall provide Computer Incident Response Team (CIRT) services. The contractor shall adhere to the standard Incident Reporting process as determined by the Component and is defined by a DHS-specific incident response plan that adheres to DHS policy and procedure for reporting incidents. The contractor shall conduct Incident Response Exercises to ensure all personnel are familiar with the plan. The contractor shall notify the DHS SOC of any incident in accordance with the Incident Response Plan and work with DHS throughout the incident duration.

Firewall Management and Monitoring

The Contractor shall provide firewall management services that include the design, configuration, implementation, maintenance, and operation of all firewalls within the hosted DHS infrastructure in accordance with DHS architecture and security policy. The contractor shall provide all maintenance to include configuration, patching, rule maintenance (add, modify, delete), and comply with DHS' configuration management / release management requirements when changes are required. Firewalls shall operate 24x7x365. Analysis of the firewall logs shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Intrusion Detection Systems and Monitoring

The Contractor shall provide the design, configuration, implementation, and maintenance of the sensors and hardware that are required to support the NIDS solution. The contractor is responsible for creating and maintaining the NIDS rule sets. The NIDS

U.S. Customs and Border Protection

Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

solution should provide real-time alerts. These alerts and other relevant information shall be located in a central repository. The NIDS shall operate 24x7x365. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Physical and Information Security and Monitoring

The Contractor shall provide a facility using appropriate protective measures to provide for physical security. The facility will be located within the United States and its territories. The contractor shall maintain a process to control physical access to DHS IT assets. DHS IT Assets shall be monitored 24x7x365. A summary of unauthorized access attempts shall be reported to the appropriate DHS security office.

Vulnerability Assessments

The Contractor shall provide all information from any managed device to DHS, as requested, and shall assist, as needed, to perform periodic vulnerability assessments of the network, operating systems, and applications to identify vulnerabilities and propose mitigations. Vulnerability assessments shall be included as part of compliance with the continuous monitoring of the system.

Anti-malware (e.g., virus, spam)

The Contractor shall design, implement, monitor and manage to provide comprehensive anti-malware service. The contractor shall provide all maintenance for the system providing the anti-malware capabilities to include configuration, definition updates, and comply with DHS' configuration management / release management requirements when changes are required. A summary of alerts shall be reported to DHS COR in weekly status reports. If an abnormality or anomaly is identified, the contractor shall notify the appropriate DHS point of contact in accordance with the incident response plan.

Patch Management

The Contractor shall perform provide patch management services. The contractor shall push patches that are required by vendors and the DHS system owner. This is to ensure that the infrastructure and applications that directly support the DHS information system are current in their release and that all security patches are applied. The contractor shall be informed by DHS which patches that are required by DHS through the Information Security Vulnerability Management bulletins and advisories. Core applications, the ones DHS utilizes to fulfill their mission, shall be tested by DHS. However, the contractor shall be responsible for deploying patches as directed by DHS. It is recommended that all other applications (host-based intrusion detection system (HIDS), network intrusion detection system (NIDS), Anti-malware, and Firewall) shall be tested by the contractor prior to deployment in a test environment.

Log Retention

Log files for all infrastructure devices, physical access, and anti-malware should be retained online for 180 days and offline for three years.

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade
Supply Chain Risk Management Requirement

Supply Chain risks result from adversarial exploitation of the organizations, people, activities, information, resources, or facilities that provide hardware, software, or services. These risks can result in a loss of confidentiality, integrity, or availability of information or information systems. A compromise to even minor system components can lead to adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Authorities:

Comprehensive National Cybersecurity Initiative (CNCI) Initiative 11, Develop Multi-Pronged Approach for Global Supply Chain Risk Management

Department of Homeland Security, Security Policy for Sensitive Systems 4300A

Homeland Security Presidential Directive 23, Cyber Security and Monitoring, 8 January 2008

Office of Budget and Management Circulation A-130, Appendix III

•National Institute of Standards and Technology, Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013

Supply Chain Risk Management

The Contractors supplying the Government hardware and software shall provide the manufacture's name, address, state and/or domain of registration, and the Data Universal Numbering System (DUNS) number for all components comprising the hardware and software. If subcontractors or subcomponents are used, the name, address, state and/or domain of registration and DUNs number of those suppliers must also be provided.

Subcontractors are subject to the same general requirements and standards as prime contractors. Contractors employing subcontractors shall perform due diligence to ensure that these standards are met.

The Government shall be notified when a new contractor/subcontractor/service provider is introduced to the supply chain, or when suppliers of parts or subcomponents are changed.

Contractors shall provide, implement, and maintain a Supply Chain Risk Management Plan that addresses internal and external practices and controls employed to minimize the risk posed by counterfeits and vulnerabilities in systems, components, and software.

The Plan shall describe the processes and procedures that will be followed to ensure appropriate supply chain protection of information system resources developed, processed, or used under this contract.

The Supply Chain Risk Management Plan shall address the following elements:

1. How risks from the supply chain will be identified,

U.S. Customs and Border Protection

Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

2. What processes and security measures will be adopted to manage these risks to the system or system components, and
3. How the risks and associated security measures will be updated and monitored.

The Supply Chain Risk Management Plan shall remain current through the life of the contract or period of performance. The Supply Chain Risk Management Plan shall be provided to the Contracting Officer Technical Representative (COR) 30 days post award.

The Contractor acknowledges the Government's requirement to assess the Contractors Supply Chain Risk posture. The Contractor understands and agrees that the Government retains the right to cancel or terminate the contract, if the Government determines that continuing the contract presents an unacceptable risk to national security.

The Contractor shall disclose, and the Government will consider, relevant industry standards certifications, recognitions and awards, and acknowledgments.

The Contractor shall provide only new equipment unless otherwise expressly approved, in writing, by the Contracting Officer (CO). Contractors shall only provide Original Equipment Manufacturers (OEM) parts to the Government. In the event that a shipped OEM part fails, all replacement parts must be OEM parts.

The Contractor shall be excused from using new OEM (i.e. "grey market," previously used) components only with formal Government approval. Such components shall be procured from their original genuine source and have the components shipped only from manufacturers authorized shipment points.

For software products, the contractor shall provide all OEM software updates to correct defects for the life of the product (i.e. until the "end of life."). Software updates and patches must be made available to the government for all products procured under this contract.

Contractors shall employ formal and accountable transit, storage, and delivery procedures (i.e., the possession of the component is documented at all times from initial shipping point to final destination, and every transfer of the component from one custodian to another is fully documented and accountable) for all shipments to fulfill contract obligations with the Government.

All records pertaining to the transit, storage, and delivery will be maintained and available for inspection for the lessor of the term of the contract, the period of performance, or one calendar year from the date the activity occurred.

These records must be readily available for inspection by any agent designated by the US Government as having the authority to examine them.

This transit process shall minimize the number of times en route components undergo a change of custody and make use tamper-proof or tamper-evident packaging for all shipments. The supplier, at the Government's request, shall be able to provide shipping status at any time during transit.

The Contractor is fully liable for all damage, deterioration, or losses incurred during shipment and handling, unless the damage, deterioration, or loss is due to the

U.S. Customs and Border Protection
Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

Government. The Contractor shall provide a packing slip which shall accompany each container or package with the information identifying the contract number, the order number, a description of the hardware/software enclosed (Manufacturer name, model number, serial number), and the customer point of contact. The contractor shall send a shipping notification to the intended government recipient or contracting officer. This shipping notification shall be sent electronically and will state the contract number, the order number, a description of the hardware/software being shipped (manufacturer name, model number, serial number), initial shipper, shipping date and identifying (tracking) number.

4.1.3.8 Personal Identification Verification (PIV) Credential Compliance

Authorities:

- HSPD-12 “Policies for a Common Identification Standard for Federal Employees and Contractors”
- OMB M-11-11 "Continued Implementation of Homeland Security Presidential Directive (HSPD) 12– Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB M-06-16 “Acquisition of Products and Services for Implementation of HSPD-12”
- NIST FIPS 201 “Personal Identity Verification (PIV) of Federal Employees and Contractors”
- NIST SP 800-63 “Electronic Authentication Guideline”
- OMB M-10-15 “FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management”

Personal Identification Verification (PIV) Credential Compliance Requirement

Procurements for products, systems, services, hardware, or software involving controlled facility or information system shall be PIV-enabled by accepting HSPD-12 PIV credentials as a method of identity verification and authentication.

Procurements for software products or software developments shall be compliant by PIV by accepting PIV credentials as the common means of authentication for access for federal employees and contractors.

PIV-enabled information systems must demonstrate that they can correctly work with PIV credentials by responding to the cryptographic challenge in the authentication protocol before granting access.

If a system is identified to be non-compliant with HSPD-12 for PIV credential enablement, a remediation plan for achieving HSPD-12 compliance shall be required for review, evaluation, and approval by the CISO.

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade
**Security Requirements for Unclassified Information Technology Resources
Requirement**

Contractor Employee Access Clause

As prescribed in (HSAR) 48 CFR 3004.470-3 Contract clauses, insert a clause substantially the same as follows:

(b) Contracting officers shall insert the basic clause at (HSAR) 48 CFR 3052.204-71, Contractor Employee Access, in solicitations and contracts when contractor employees require recurring access to Government facilities or access to sensitive information. Contracting officers shall insert the basic clause with its Alternate I for acquisitions requiring contractor access to IT resources. For acquisitions in which the contractor will not have access to IT resources, but the Department has determined contractor employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, the contracting officer shall insert the clause with its Alternate II. Neither the basic clause nor its alternates shall be used unless contractor employees will require recurring access to Government facilities or access to sensitive information. Neither the basic clause nor its alternates should ordinarily be used in contracts with educational institutions.

3052.204-70 Security requirements for unclassified information technology resources.
SECURITY REQUIREMENTS FOR UNCLASSIFIED INFORMATION TECHNOLOGY RESOURCES (JUN 2006)

(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission.

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract.

(1) Within 30 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(2) The Contractor's IT Security Plan shall comply with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.); the Government Information Security Reform Act of 2000; and the Federal Information Security Management Act of 2002; and with Federal policies and procedures that include, but are not limited to, OMB Circular A-130.

U.S. Customs and Border Protection
Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

- (3) The security plan shall specifically include instructions regarding handling and protecting sensitive information at the Contractor's site (including any information stored, processed, or transmitted using the Contractor's computer systems), and the secure management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems.
- (c) Examples of tasks that require security provisions include—
- (1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
- (2) Access to DHS networks or computers at a level beyond that granted the general public (e.g., such as bypassing a firewall).
- (d) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and certify that all non-public DHS information has been purged from any contractor-owned system. Components shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.
- (e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

3052.204-71 Contractor employee access.

**CONTRACTOR EMPLOYEE
ACCESS (SEP 2012)**

(a) Sensitive Information, as used in this clause, means any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security interest, the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. This definition includes the following categories of information:

- (1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Pub. L. 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade

- (2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, "Policies and Procedures of Safeguarding and Control of SSI," as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);
- (3) Information designated as "For Official Use Only," which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and
- (4) Any information that is designated "sensitive" or subject to other controls, safeguards or protections in accordance with subsequently adopted homeland security information handling procedures.
- (b) "Information Technology Resources" include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.
- (c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All Contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.
- (d) The Contracting Officer may require the Contractor to prohibit individuals from working on the contract if the Government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.
- (e) Work under this contract may involve access to sensitive information. Therefore, the Contractor shall not disclose, orally or in writing, any sensitive information to any person unless authorized in writing by the Contracting Officer. For those Contractor employees authorized access to sensitive information, the Contractor shall ensure that these persons receive training concerning the protection and disclosure of sensitive information both during and after contract performance.
- (f) The Contractor shall include the substance of this clause in all subcontracts at any tier where the subcontractor may have access to Government facilities, sensitive information, or resources.

U.S. Customs and Border Protection

Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

Alternate I (SEP 2012) When the contract will require Contractor employees to have access to Information Technology (IT) resources, add the following paragraphs:

(g) Before receiving access to IT resources under this contract the individual must receive a security briefing, which the Contracting Officer's Technical Representative (COR) will arrange, and complete any nondisclosure agreement furnished by DHS.

(h) The Contractor shall have access only to those areas of DHS information technology resources explicitly stated in this contract or approved by the COR in writing as necessary for performance of the work under this contract. Any attempts by Contractor personnel to gain access to any information technology resources not expressly authorized by the statement of work, other terms and conditions in this contract, or as approved in writing by the COR, is strictly prohibited. In the event of violation of this provision, DHS will take appropriate actions with regard to the contract and the individual(s) involved.

(i) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the Contractor performs business for the DHS Component. It is not a right, a guarantee of access, a condition of the contract, or Government Furnished Equipment (GFE).

(j) Contractor access will be terminated for unauthorized use. The Contractor agrees to hold and save DHS harmless from any unauthorized use and agrees not to request additional time or money under the contract for any delays resulting from unauthorized use or access.

(k) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Component or designee, with the concurrence of both the Department's Chief Security Officer (CSO) and the Chief Information Officer (CIO) or their designees. Within DHS Headquarters, the waiver may be granted only with the approval of both the CSO and the CIO or their designees. In order for a waiver to be granted:

(1) There must be a compelling reason for using this individual as opposed to a U.S. citizen; and

(2) The waiver must be in the best interest of the Government.

(l) Contractors shall identify in their proposals the names and citizenship of all non-U.S. citizens proposed to work under the contract. Any additions or deletions of non-U.S. citizens after contract award shall also be reported to the Contracting Officer.

System Security documentation appropriate for the SDLC status

U.S. Customs and Border Protection
Statement of Work (SOW)
Splunk Enterprise Logging Maintenance Renewal & Upgrade
Security Certification/Accreditation

CBP Program Offices shall provide personnel (System Owner and Information System Security Officers) with the appropriate clearance levels to support the security certification/accreditation processes under this Agreement in accordance with the current version of the DHS MD 4300A, DHS Sensitive Systems Policy and Handbook, CBP Information Systems Security Policies and Procedures Handbook HB-1400-05, and all applicable National Institute of Standards and Technology (NIST) Special Publications (800 Series). During all SDLC phases of CBP systems, CBP personnel shall develop documentation and provide any required information for all levels of classification in support of the certification/accreditation process. In addition, all security certification/accreditation will be performed using the DHS certification/accreditation process, methodology and tools. An ISSO performs security actions for an information system. There is only one ISSO designated to a system, but multiple Alternate ISSOs may be designated to assist the ISSO. While the ISSO performs security functions, the System Owner is always responsible for information system security (4300A). System owners shall include information security requirements in their capital planning and investment control (CPIC) business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS information system. System owners or AOs shall ensure that information security requirements and POA&Ms are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.

Disaster Recovery Planning & Testing – Hardware

If the system owner requires a robust DR solution (full redundancy and failover capabilities (for near zero downtime)) then the funded DR solution must match the production environment like-for-like. This solution would also include additional software licenses, hardware, firmware and storage for the DR environment.

The system owner or program office must also include travel, per diem and approximately 16 over the core hours for travel to recovery facilities twice per fiscal year for system administrators, DBA's, end users or testers

If the system owner requires a moderate DR solution that would provide a working environment that is capable of handling their mission essential functions then they can fund a scaled down solution which should still take into consideration additional hardware, software licenses, and storage for the DR environment.

The system owner or program office is still responsible for the costs associated with testing their DR solution; however, for a scaled down solution, it may be possible to leverage or share staff already designated to participate in DR activities.

If the system owner only requires a low DR solution then the system owner or program office can use internal resources to perform a table-top exercise, which generally does not require travel, additional hardware or software licenses.

Engineering Platforms

U.S. Customs and Border Protection

Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

Common Enterprise Services (CES) – Deliver the systems, infrastructure, and operational capabilities to fully implement the three service levels defined as part of the DHS/CBP Common Enterprise Services and support DHS Component use of those services. This includes the build out and integration of all required services and infrastructure, which must include the Single Sign-on Portal and CBP Enterprise Services Bus (ESB), required for the CES. Capabilities shall be designed to the DHS standard operating architecture (SOA), transportable between DHS data centers (CBP National Data Center, Stennis, and DHS 2nd data center).

Single Sign-on Portal – Design, build, and operate a single sign-on Portal - consistent with DHS' enterprise portal solution (for which ICE is the steward) - to provide a common point of access, with a single sign-on capability to existing applications and to provide the infrastructure for integrating diverse internal and/or external information and transactional resources. This includes the migration of the current ACE Portal to the Single Sign-on Portal as rapidly as feasible.

Help Desk and Operations Support

The Contractor shall provide third tier reporting for trouble calls received from the Help Desk, the DHS Task Manager, or the users. The Contractor shall respond to the initiators of trouble calls as by receiving telephonic notifications of problems, resolving them, or directing them to the proper technical personnel for resolution. Problems that cannot be resolved immediately or with the requirements of the performance standards are to be brought to the attention of the DHS Task Manager. The Contractor shall document notification and resolution of problems in Remedy.

Interfacing

As requested by the COR, assistance in consolidating all systems with the DHS Consolidated Data Center. Resources to be consolidated with the DHS Consolidated Data Center for each system are to be determined by the COR.

Transition Plan

The DHS CIO has established portfolio targets for the IT infrastructure that include production system consolidation at a DHS data center, and transition to OneNet. The Contractor must be prepared to support CBP government leads, within the purview of this task order, to provide any required transition planning or program execution, associated with meeting the agreed to transition timeline, as directed by Government personnel. This includes the following types of tasking:

- Coordination with Government representatives
- Review, evaluation and transition of current support services
- Transition of historic data to new Contractor system
- Government-approved training and certification process
- Transfer of all necessary business and/or technical documentation

U.S. Customs and Border Protection

Statement of Work (SOW)

Splunk Enterprise Logging Maintenance Renewal & Upgrade

- Orientation phase and program to introduce Government personnel, programs, and users to the Contractor's team, tools, methodologies, and business processes, equipment, furniture, phone lines, computer equipment, etc.
- Transfer of Government Furnished Equipment (GFE) and Government Furnished Information (GFI), and GFE inventory management assistance
- Applicable debriefing and personnel out-processing procedures